BRAVATEK
TECHNICAL NOTE 2

PREVENTING EMAIL PHISHING ATTACKS USING ECRYPT ONE

Introduction

Phishing attacks continue to rise in frequency and complexity. The most recent high-profile example is the OPM attack although the attack on the RSA and its fallout was also significant. Bad actors see the human as the easiest way past all the defences that organizations put in place to secure their systems. Using Ecrypt One's email server with built-in anti-phishing features gives IT the control to eliminate this means of attack.

Problem Description

Phishing is becoming a greater and greater concern for all IT organizations, since protecting against it traditionally relies on the judgement of humans. As the security strength of other security tools increases, the weakest link can expect to be increasingly the target of attack. US-CERT, Lifehacker and other dedicated awareness programs all attempt to educate and train users to identify phishing. However, it only takes one well-crafted message to through for an attack on an organization to be successful. Time is on the side of the bad guys – they can improve the quality of their attacks and they are not going to go away while such easy targets are available to them. At the same time, most companies leave users open to email from any sender, relying on spam detectors and antivirus to detect malicious messages.

Solution

A key part of Ecrypt One's security features is its whitelist approach. Much like a firewall, Ecrypt One allows IT to define external users and domains the organization trusts and how much. Levels of trust are configurable by the administrator. By default, Ecrypt One blacklists email from the entire Internet, then lets you add who you allow. This immediately eliminates your users as phishing targets.

You can define only who you trust and only who in your organization needs to have broader trust (Support, Marketing) and who has less external contact (Engineering, Finance). By restricting external email to those you trust for most users, you can eliminate the phishing emails from ever getting to them.

You can turn up the trust for an external user or entire domain by allowing the messages to come in but have the attachments converted to more benign PDF and the message body converted to plain text. Most phishing attacks are in the form of documents with script in them, so by converting

Related Information

You can find out more about Ecrypt One at www.ecryptone.com

About Bravatek Solutions

Bravatek Solutions is a high technology security solutions portfolio provider that assists corporate entities, governments and individuals protect their organizations against both physical and cyber-attacks through its offering of the most technically-advanced, cost-effective and reliable software, tools and systems.

www.bravatek.com

to PDF, the execution of the script is destroyed. Phishing messages can also include hidden elements in an HTML-format message, so by converting to plain text, those links and external image callbacks to the outside are eliminated. You could even open up your organization to email from the entire Internet and these two measures would eliminate all direct means of phishing. The amount of protection you need and use is up to you.

Related Information

You can find out more about Ecrypt One at www.ecryptone.com

About Bravatek Solutions

Bravatek Solutions is a high technology security solutions portfolio provider that assists corporate entities, governments and individuals protect their organizations against both physical and cyber-attacks through its offering of the most technically-advanced, cost-effective and reliable software, tools and systems.

www.bravatek.com